

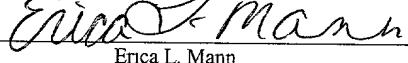
PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re the application of )  
Schweitzer et al. ) Group Art Unit: Unassigned  
Application No. Unassigned ) Examiner: Unassigned  
Filed: Herewith ) Attorney Docket No. XACTP014C  
For: DATABASE MANAGEMENT AND )  
RECOVERY IN A NETWORK- ) Date: August 21, 2001  
BASED FILTERING AND )  
AGGREGATING PLATFORM )  
(as amended) )

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as Express Mail in an envelope addressed to: Assistant Commissioner for Patents, Washington, DC 20231 on August 21, 2001.

Signed:   
Erica L. Mann

PRELIMINARY AMENDMENT

Commissioner for Patents  
Washington, DC 20231

Dear Sir:

Prior to substantive Examination of the above-identified patent application, please enter the following amendments.

IN THE TITLE:

Please delete the TITLE OF THE INVENTION, and insert a new TITLE OF THE INVENTION as set forth hereinbelow:

--DATABASE MANAGEMENT AND RECOVERY IN A NETWORK-BASED FILTERING AND AGGREGATING PLATFORM--.

IN THE SUMMARY:

Please delete the SUMMARY OF THE INVENTION, and insert a new SUMMARY OF THE INVENTION as set forth hereinbelow: (See Appendix A)

A system with accompanying method and computer program product are provided for database management and recovery. Included are information source modules for collecting network communications usage information in real-time from a plurality of network devices. Also included is a plurality of gatherers coupled to the information source modules. The gatherers are adapted for filtering and aggregating the network communications usage information. A central event manager is coupled to the gatherers for completing a plurality of data records from the filtered and aggregated network communications usage information. Such data records correspond to network usage by a plurality of users. A database is coupled to the central event manager for storing the data records. Further provided is logic for continuously monitoring a state of the gatherers, detecting a fault, and utilizing the state of the gatherers and the stored data records to recover from the fault upon the detection thereof.

IN THE ABSTRACT:

Please delete the ABSTRACT OF THE INVENTION, and insert a new ABSTRACT OF THE INVENTION as set forth hereinbelow: (See Appendix B)

A system with accompanying method and computer program product are provided for database management and recovery. Included are information source modules for collecting network communications usage information in real-time from a plurality of network devices. Also included is a plurality of gatherers coupled to the information source modules. The gatherers are adapted for filtering and aggregating the network communications usage information. A central event manager is coupled to the gatherers for completing a plurality of data records from the filtered and aggregated network communications usage information. Such data records correspond to network usage by a plurality of users. A database is coupled to the central event manager for storing the data records. Further provided is logic for continuously monitoring a state of the gatherers, detecting a fault, and utilizing the state of the gatherers and the stored data records to recover from the fault upon the detection thereof.

IN THE CLAIMS:

Please cancel claims 1-31, and add claims 32-47, as follows:

32. A method for database management and recovery, comprising:

- (a) collecting network communications usage information in real-time from a plurality of network devices utilizing a plurality of information source modules;
- (b) filtering and aggregating the network communications usage information utilizing a plurality of gatherers;
- (c) completing a plurality of data records from the filtered and aggregated network communications usage information utilizing a central event manager, the plurality of data records corresponding to network usage by a plurality of users;
- (d) storing the data records in a database;
- (e) continuously monitoring a state of the gatherers;
- (f) detecting a fault; and
- (g) utilizing the state of the gatherers and the stored data records to recover from the fault upon the detection thereof.

33. A method as recited in claim 32, wherein the data records are stored in the database at a user-specified interval.

34. A method as recited in claim 32, and further comprising time stamping the stored data records.

35. A method as recited in claim 34, and further comprising deleting the stored data records upon the cessation of a predetermined amount of time after the storage utilizing the timestamp.

36. A method as recited in claim 32, and further comprising caching the network communications usage information collected from the network device utilizing the gatherers.

37. A computer program product for database management and recovery, comprising:

- (a) computer code for collecting network communications usage information in real-time from a plurality of network devices utilizing a plurality of information source modules;
- (b) computer code for filtering and aggregating the network communications usage information utilizing a plurality of gatherers;
- (c) computer code for completing a plurality of data records from the filtered and aggregated network communications usage information utilizing a central event manager, the plurality of data records corresponding to network usage by a plurality of users;
- (d) computer code for storing the data records in a database;
- (e) computer code for continuously monitoring a state of the gatherers;
- (f) computer code for detecting a fault; and
- (g) computer code for utilizing the state of the gatherers and the stored data records to recover from the fault upon the detection thereof.

38. A computer program product as recited in claim 37, wherein the data records are stored in the database at a user-specified interval.

39. A computer program product as recited in claim 37, and further comprising computer code for time stamping the stored data records.

40. A computer program product as recited in claim 39, and further comprising computer code for deleting the stored data records upon the cessation of a predetermined amount of time after the storage utilizing the timestamp.

41. A computer program product as recited in claim 37, and further comprising computer code for caching the network communications usage information collected from the network devices utilizing the gatherers.

42. A system for database management and recovery, comprising:

- (a) information source modules for collecting network communications usage information in real-time from a plurality of network devices;
- (b) gatherers coupled to the information source modules, the gatherers adapted for filtering and aggregating the network communications usage information;
- (c) a central event manager coupled to the gatherers, the central event manager adapted for completing a plurality of data records from the filtered and aggregated network communications usage information, the plurality of data records corresponding to network usage by a plurality of users;
- (d) a database coupled to the central event manager, the database adapted for storing the data records;
- (e) logic for continuously monitoring a state of the gatherers;
- (f) logic for detecting a fault; and
- (g) logic for utilizing the state of the gatherers and the stored data records to recover from the fault upon the detection thereof.

43. A system as recited in claim 42, wherein the data records are stored in the database at a user-specified interval.

44. A system as recited in claim 42, and further comprising computer code for time stamping the stored data records.

45. A system as recited in claim 44, and further comprising computer code for deleting the stored data records upon the cessation of a predetermined amount of time after the storage utilizing the timestamp.

46. A system as recited in claim 42, and further comprising computer code for caching the network communications usage information collected from the network devices utilizing the gatherers.

47. A method for reporting on the collection of network usage information from a plurality of network devices, the method comprising:

- (a) collecting network communications usage information in real-time from network devices at a plurality of layers utilizing multiple gatherers each including a plurality of information source modules each interfacing with one of the network devices and capable of communicating using a protocol specific to the network device coupled thereto, the network devices selected from the group consisting of routers, switches, firewalls, authentication servers, web hosts, proxy servers, netflow servers, databases, mail servers, RADIUS servers, and domain name servers, the gatherers being positioned on a segment of the network on which the network devices coupled thereto are positioned for minimizing an impact of the gatherers on the network;
- (b) translating the network communications usage information collected from the network devices utilizing the information source modules;
- (c) caching the network communications usage information collected from the network devices utilizing the gatherers;
- (d) normalizing the network communications usage information with the gatherers by excluding fields not required by a central event manager coupled to the gatherers;
- (e) defining an enhancement procedure utilizing the central event manager;
- (f) coordinating the collection of the network communications usage information by the gatherers utilizing the central event manager;
- (g) filtering the network communications usage information utilizing the central event manager;
- (h) completing a plurality of data records from the filtered network communications usage information, the plurality of data records corresponding to network usage by a plurality of users;
- (i) aggregating the network communications usage information and the data records utilizing the central event manager for reducing a number of the data records;
- (j) enhancing the aggregation with the gatherers in accordance with the defined enhancement procedure;
- (k) time stamping the data records;
- (l) storing the time stamped data records in tables in a central database coupled to the central event manager at a user-specified interval; and
- (m) deleting the stored data records upon the cessation of a predetermined amount of time after the storage utilizing the timestamp.

REMARKS

The claims of the present application have been amended to include subject matter clearly disclosed in the originally filed specification. No new matter has been added.

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 505-5100. For payment of the fees due in connection with the filing of this paper, the Commissioner is authorized to charge such fees to Deposit Account No. 50-1351 (Order No. XACTP014C). A duplicate copy of the transmittal is enclosed for this purpose.

Respectfully submitted,

Kevin J. Zilka  
Registration No. 41,429

P.O. Box 721120  
San Jose, CA 95172-1120  
408-505-5100